



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/422,196	10/21/1999	DIMITRI KANEVSKY	12835-(YO999	5233

7590 02/24/2004

RICHARD L CATANIA ESQ  
SCULLY SCOTT MURPHY AND PRESSER  
400 GARDEN CITY PLAZA  
GARDEN CITY, NY 11530

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 02/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/422,196

Applicant(s)

KANEVSKY ET AL.

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 12/11/03.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-52 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-52 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims ~~4-52~~<sup>1-15, 17-36, 38-52</sup> are rejected under 35 U.S.C. 102(e) as being anticipated by Schneck (US 6, 314, 409 B2).

a. Referring to claim 1:

i. Schneck teaches:

(1) means for determining fulfillment of one or more certain conditions at said destination location [i.e., **Figure 5, package rules 152, the access mechanism 114 allows a user 104 to access the data in packaged data according to the rules provided with (as package rules 152) the packaged data and prevents the user or anyone else from accessing the data other than as allowed by the rules (column 15, line 31-35)]**, said means including means enabling a sender of a communicated package to observe a user requesting access to content at said destination location, said condition including sender identification of said user [i.e., **the data are being accessed by an application via an insecure operating system (OS) which invokes the access mechanism 114. The intent is to show the manner in which controlled access of the data takes place. In some foreseen environments, the operating system will be little more than a simple runtime system or there will be only one program running at all times. For example, in a video cassette recorder and playback machine (VCR), a single control program may be running at all times to control the VCR's operations, that is "to observe a**

user requesting access to content". In this case, this control program is considered the application, and all access to controlled data is initiated by the control program which invokes the access mechanism 114 (column 18, lines 5-17)]. Furthermore, the access mechanism may allow the owner to place a global set of rules (a global permission list) in the mechanism. These global rules could control, for example, hours of access (e.g., when the computer might be operated) based on a clock within the access mechanism or an external time reference with which the access mechanism communicates; acceptable software which can be run using the access mechanism (i.e., a list of those software products that would be allowed to be used, thus enforcing a system administrator's configuration control rules); user (that is "sender identification") and password lists, and the like. A user can thereby customize a particular access mechanism. The rules may also include or specify certain programs to be run under certain conditions (column 32, lines 31-44)]; and

(2) control means responsive to detection of a fulfilled one or more certain conditions for enabling access to content provided in a communicated package, whereby said access includes enabling a user to perform an operation on said package content at said destination location [i.e., all components of the access mechanism are packaged in such a way as to exclude any unknown access by a user and to discover any such attempt at user access to the components or their contents. That is, the access mechanism is packaged in a tamper-detectable manner, and, once tampering is detected, the access mechanism is disable (column 15, line 62-67)].

b. Referring to claim 2 which depends on claim 1:

i. Schneck further teaches:

(1) wherein said electronic information packages include content comprising one or more of: e-mail messages, audio data, video data, animation data, textual data, and pictorial data [i.e., Figure 15, data 106, digitally stored information may include binary data, computer software, text, graphics, audio, video, and the like, alone or in combination (column 10, line 6-9)].

c. Referring to claim 3 which depends on claim 2:

i. Schneck further teaches:

(1) means for automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions **[i.e., tamper detection allows the access mechanism to ensure that all internal data (both the system's data and any user data) are destroyed before any tamperer can obtain them (column 16, line 27-30)]**.

d. Referring to claim 4 which depends on claim 3:

i. Schneck further teaches:

(1) wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals, said system further comprising means for determining elapsed time from receipt of an electronic information package, said means generating a signal for destroying the received electronic information package after a time interval has elapsed **[i.e., control of expiration dates, time of use, number and frequency of uses and permitted users. For example, rights to use a file of data (whatever it contains) may expire on a certain date; access to certain data may be limited to certain time of day, days of week or specific dates (column 31, line 1-5); tamper detection allows the access mechanism to ensure that all internal data (both the system's data and any user data) are destroyed before any tamperer can obtain them (column 16, line 27-30)]**.

e. Referring to claim 5 which depends on claim 4:

i. Schneck further teaches:

(1) wherein said elapsed time interval is specified by a sender at said sending device, said electronic information package further comprising a specification of one or more time-out intervals for use by said elapsed timing means **[i.e., a user may only be allowed to access certain data a specified number of times, or a specified number of times per day (column 31, line 6-7)]**.

f. Referring to claim 6 which depends on claim 5:

i. This claim has limitations that are similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

g. Referring to claim 7 which depends on claim 5:

i. Schneck further teaches:

(1) wherein said operations enabled to be performed on said package content at said destination device include playing audio data on one or several speakers at said destination location **[i.e., the display or output devices used will depend on the application, and the type of data, and include, but are not limited to printers, video display monitor, audio output devices, and the like (column 17, line 37-40)]**.

h. Referring to claim 8 which depends on claim 3:

i. Schneck further teaches:

(1) wherein said access includes forbidding a user to perform an operation on said package content at said destination device, said operations that are forbidden to be performed on received information packages include one or more of: saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location **[i.e., some parameters are independent of any other parameters; some parameters are mutually exclusive; and other parameters must be used in combination to define fully the actions to be allowed or disallowed: no modify, no copy, no print, no execute, no access, etc. (column 23, line 13-45)]**.

i. Referring to claims 9, 25, 30, 42, and 44:

i. These claims have limitations that are similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

j. Referring to claim 10 which depends on claim 8:

i. Schneck further teaches:

(1) wherein said means for determining fulfillment of one or more certain conditions at said destination device further includes means for receiving a direct command signal from a sender at a sending device, said sender command triggering destruction of said electronic information package **[i.e., the rules can specify various access rights and controls, including rights of further**

**distribution of the data, which are destroyed when tampering is detected (column 7, line 55-60)].**

k. Referring to claim 11 which depends on claim 8:

i. Schneck further teaches:

(1) wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, said physical hardware devices including CPU, memory or peripherals at said destination device, said destroying means automatically destroying a received electronic information package in response to said detection **[i.e., the coprocessor is protected by tamper detection that causes the rules, cryptographic data, and decrypted protected data to be destroyed. Both passive and active means are used to effect such destruction. Semiconductor memory is volatile and does not retain data when power is removed (column 8, line 39-44)].**

l. Referring to claims 12, 26, 33, 43, and 47:

i. These claims have limitations that are similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

m. Referring to claim 13:

i. Schneck further teaches:

(1) wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages **[i.e., the operating system is notified of the termination of each program so that it may close any files opened by the program. Because it is possible that multiple programs may be executing at the same time, the system will remain in a protected state until all active programs conclude their execution (column 19, line 15-20)].**

n. Referring to claim 14 which depends on claim 9:

i. Schneck further teaches:

(1) wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting a pressing of a key on a keyboard operable for said destination device [**i.e., degrees of protection utilized in the computer system hardware (for example, tamperproof and tamper-detect features) and the cryptographic tools will depend on the nature of the data to be protected as well as the user environment (column 7, line 10-14)]**].

o. Referring to claim 15 which depends on claim 1:

i. Schneck further teaches:

(1) wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying a user at said destination location for which access to these information packages is allowed [**i.e., Figure 3, token/biometrics 146 indicates the physical tokens and/or biometric characteristics (if any) required for identification of each authorized user (column 11, line 40-44)]**].

p. Referring to claim 17 which depends on claim 15:

i. Schneck further teaches:

(1) wherein said identification means for identifying a user at said destination location comprises:

(a) means for enabling users to present a password to said system [**i.e., the invention can be used in combination with software and other identification technology to limit data access to users that possess an appropriate physical or logical token (for example, a dongle or password) (column 24, line 66-67 and column 25, line 1-3)]**; and,

(b) verification means for verifying a user's password prior to enabling access to said information package [**i.e., permission list consists of rules governing the qualities and quantities of access made available**].



by the owner to a particular user or group or class of users, and defines those ways in which the user may (and may not) interact with the owner's data/information (column 23, line 66-67 and column 24, line 1-3)].

q. Referring to claim 18 which depends on claim 15:

i. Schneck further teaches:

(1) wherein said identification means for identifying a user at said destination location comprises means for enabling users to present a data for authentication/verification that include one or more of the following: biometrics, fingerprint, and voice data [i.e., **other identification technology (for example, biometric sensors) or personal characteristic (for example, a fingerprint pattern)** (column 24, line 67 and column 25, line 3-4)].

r. Referring to claim 19 which depends on claim 1:

i. Schneck further teaches:

(1) wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying an electronic system at said destination location for which access to these information packages is allowed [i.e., **may be limited to a particular computer system, a particular token (such as a smart card)** (column 24, line 11-12)].

s. Referring to claim 20 which depends on claim 19:

i. Schneck further teaches:

(1) wherein said electronic system trying to access information packages comprises a communication process that supports transferring electronic package content via a communication channel to new destination locations [i.e., **Figure 1, the data distributor 102 takes data 106 and produces packaged data 108 which are provided to the user 104 via communication channel 105** (column 9, line 55-57)].

t. Referring to claim 21 which depends on claim 19:

i. Schneck further teaches:

(1) wherein said electronic system trying to access information packages comprises an automated process capable of understanding

Art Unit: 2135

information package content and performing necessary operations as required for playing said content [i.e., **the entire process can be automated (column 30, line 7)**].

u. Referring to claim 22 which depends on claim 19:

i. Schneck further teaches:

(1) wherein said electronic system trying to access information packages comprises a robotic device [i.e., **computer control of processes is basis for automation and quality control in many industries. This technology extends into various specialties such as robotics, robotic programming languages, etc. (column 31, line 34-40)**].

v. Referring to claim 23 which depends on claim 1:

i. Schneck further teaches:

(1) wherein said electronic information packages communicated from a sending device to a device at one or more destination locations, is communicated over a communications channel including one or more of: telephone wires, wireless channels, radio links, network data connection [i.e., **data provided to user may be provided and distributed in various ways, including but not limited to, via digital communications networks (for example the internet), magnetic media, CD-ROM, semiconductor memory modules, and wireless (column 15, line 10-19)**].

w. Referring to claims 24 and 41:

i. These claims have limitations that are similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

x. Referring to claim 27:

i. This claim has limitations that are similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

y. Referring to claim 28:

i. This claim has limitations that are similar to those of claims 2 and 7, thus it is rejected with the same rationale applied against claims 2 and 7 above.

z. Referring to claim 29:

i. This claim has limitations that are similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

aa. Referring to claims 31 and 45:

i. These claims have limitations that are similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

ab. Referring to claims 32 and 46:

i. These claims have limitations that are similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

ac. Referring to claims 34 and 48:

i. These claims have limitations that are similar to those of claim 13, thus it is rejected with the same rationale applied against claim 13 above.

ad. Referring to claims 35 and 49:

i. These claims have limitations that are similar to those of claim 14, thus it is rejected with the same rationale applied against claim 14 above.

ae. Referring to claims 36 and 50:

i. These claims have limitations that are similar to those of claim 15, thus it is rejected with the same rationale applied against claim 15 above.

af. Referring to claims 38 and 51:

i. These claims have limitations that are similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

ag. Referring to claims 39 and 52:

i. These claims have limitations that are similar to those of claim 18, thus it is rejected with the same rationale applied against claim 18 above.

ah. Referring to claim 40:

i. This claim has limitations that are similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2135

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claim<sup>and 37 are</sup> 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Schneck (US 6, 314, 409 B2).

a. Referring to claim 16 which depends on claim 1:

i. Although Schneck does not explicitly mention the use of video camera system:

(1) wherein said means enabling a sender of a communicated package to observe a user requesting access to content includes video camera system for generating video signals at said destination device and a display device for receiving and displaying video signals at said sending device, said video camera system enabling a sender at a sending device to observe users attempting to read or play information package content at a destination device [i.e., **the data are being accessed by an application via an insecure operating system (OS) which invokes the access mechanism 114. The intent is to show the manner in which controlled access of the data takes place. In some foreseen environments, the operating system will be little more than a simple runtime system or there will be only one program running at all times. For example, in a video cassette recorder and playback machine (VCR), a single control program may be running at all times to control the VCR's operations. In this case, this control program is considered the application, and all access to controlled data is initiated by the control program which invokes the access mechanism 114 (column 18, lines 5-17). Since the control program is for controlling the VCR, it is obvious that a video camera system must be included within the system to record the image for the VCR to be able to play back the signals].**

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such video camera system in Schneck, since Schneck does mention the device containing the mechanism of the present invention can be a stand-alone device such as a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, a computer system or the like (column 7, lines 60-64)]

iii. The ordinary skilled person would have been motivated to:

(1) include such video camera system in Schneck to control access to and use and distribution of data. For example, when the data are in the form of textual and graphical information, this invention can control how much of the information is displayed and in what form (column 6, lines 63-67).

b. Referring to claim 37:

i. This claim has limitations that are similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

### ***Response to Argument***

3. Applicant's arguments filed December 11, 2003 have been fully considered but they are not persuasive.

Applicant argues that:

"Respectfully, even though the Examiner has indicated in the Office action a rejection of Claim 16, this rejection is misplaced. The Examiner indicates rejection of Claim 16 based on Schneck at Col. 8, lines 21-27, however, the indicated passage describes a tamper proof mechanism including encrypting output digital signals or scrambling analog signals, thus requiring the provision of decryption or unscrambling capability in the output device (which may include a standalone device such as a television, VCR and the like. The cited passage really does not teach or describe the mechanism as claimed in amended. Claim 16 and likewise, amended Claim 37".

Examiner maintains that:

Although Schneck does not explicitly mention video camera system, he, however, does mention the capture of output signal using output device, such as TV or monitor (column 8, lines 5-10).

Applicant further argues that:

"As Schneck does not teach the mechanism or method step for enabling the sender of the electronic information package to observe a person that requests to read or access content information at destination as now set forth in amended Claims 1, 24 and 41, it is respectfully requested that the Examiner withdraw the rejections of Claims 1, 24 and 41 as being anticipated by Schneck. Respectfully, it is further requested that the Examiner withdraw the rejection of all claims dependent upon these amended claims".

Examiner maintains that:

Schneck teaches the data are being accessed by an application via an insecure operating system (OS) which invokes the access mechanism 114. The intent is to show the manner in which controlled access of the data takes place. In some foreseen environments, the operating system will be little more than a simple runtime system or there will be only one program running at all times. For example, in a video cassette recorder and playback machine (VCR), a single control program may be running at all times to control the VCR's operations, that is "to observe a user requesting access to content". In this case, this control program is considered the application, and all access to controlled data is initiated by the control program which invokes the access mechanism 114 (column 18, lines 5-17)]. Furthermore, the access mechanism may allow the owner to place a global set of rules (a global permission list) in the mechanism. These global rules could control, for example, hours of access (e.g., when the computer might be operated) based on a clock within the access mechanism or an external time reference with which the access mechanism communicates; acceptable software which can be run using the access mechanism (i.e., a list of those software products that would be allowed to be used, thus enforcing a system administrator's configuration control rules); user (that is "sender identification") and password lists, and the like. A user can thereby customize a particular access mechanism. The rules may also include or specify certain programs to be run under certain conditions (column 32, lines 31-44).

### ***Conclusion***

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

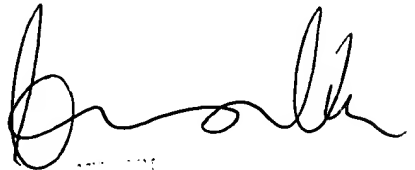
A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT  
February 9, 2003



EXAMINER  
TANYA TRUONG  
703-305-0327